Part I – Release to Press

Agenda item: ##

Meeting Cabinet

Portfolio Area Resources and Performance

Date



SHARED ICT STRATEGY 2027–2029

MATT CANTERFORD, IT DIRECTOR (SHARED ICT SERVICE)

1 PURPOSE

1.1 To present the Shared ICT Strategy 2027–2029 (attached at Appendix A) to Cabinet for consideration and approval.

1.2 To advise Members that the Joint Information and Communications Technology (ICT) Committee, comprising representatives from Stevenage Borough Council and East Herts District Council, has considered and agreed the Strategy.

1.3 To set out the key highlights of the Strategy across its three core pillars: Active Cyber Resilience, Data Intelligence & Ethical AI, and Future-Ready Tech & Culture and to confirm that the Joint Information and Communications Technology (ICT) Committee will oversee and review the Strategy in response to ongoing uncertainty around Local Government Reorganisation (LGR).

2 RECOMMENDATIONS

2.1 That Cabinet notes that the Joint Information and Communications Technology (ICT) Committee has considered and agreed the Shared ICT Strategy 2027–2029

2.2 That Cabinet approves and adopts the Shared ICT Strategy 2027–2029, including the High-Level Action Plan (2027/28), attached at Appendix A.

2.3 That Cabinet notes that the Shared ICT Strategy 2027–2029 and its High-Level Action Plan will be formally reviewed by the Joint Information and Communications Technology (ICT) Committee, ensuring the Council can adapt priorities promptly once the Government confirms its position on Local Government Reorganisation (LGR).

3 BACKGROUND

3.1 Stevenage Borough Council and East Herts District Council have operated a shared ICT Partnership since 2013. Over recent years, the role of technology in local government has evolved from a traditional back-office support function into a strategic engine that underpins frontline service delivery, resident self-service, and corporate transformation.

3.2 To fix historic underinvestment, both Councils have invested **£630,000 per year** since **2023/24** to replace outdated equipment and build a safe, reliable computer network. Now that the **Shared ICT Service** is fully staffed, these core upgrades are complete—staff computers have been updated with modern software (**Windows 11** and **Microsoft 365**), data storage is faster, and digital security defences are stronger. With these foundations in place, the service is shifting its focus from everyday IT fixes to actively improving the digital services delivered to staff and communities.

3.3 For Stevenage Borough Council, the Strategy serves as the technical bedrock for the Making Stevenage Even Better Corporate Plan (2024–2027) and the Digital Strategy 2026–2028. While the Digital Strategy defines the interactions residents experience, such as online forms, AI chatbots, and automated telephony, this ICT Strategy defines how those platforms are delivered and safely governed.

3.4 The Strategy has also been prepared in the context of Local Government Reorganisation (LGR). Following the rapid review announced on 7 September 2026 and the ministerial update on 29 October 2026, the Government confirmed that the LGR process and criteria were sound, with shadow elections scheduled for 2028 and new Unitary Authorities set to go live in 2029. With the previous July 2026 decision withdrawn, Hertfordshire awaits a final decision before Christmas 2026 or early in the New Year following further testing of existing proposals. Built on the premise that LGR will proceed, this window provides the time and capacity to audit technical debt and design flexible, modular systems that can adapt to whatever future structure is decided—or, if LGR does not happen for an extended period, to go further with deeper system integration, rationalisation into fewer systems, and shared efficiencies.

4 REASONS FOR RECOMMENDED COURSE OF ACTION AND OTHER OPTIONS

4.1 The Shared ICT Strategy 2027–2029, attached at Appendix A, sets out the shared vision and delivery framework to ensure technology continues to support officers and deliver reliable, accessible services for residents across Stevenage Borough Council and East Herts District Council. The Strategy

has been considered and agreed by the Joint Information and Communications Technology (ICT) Committee and is now presented to Cabinet for formal approval.

4.2 Rather than focusing on technical specifications which are detailed within the Strategy and High-Level Action Plan at Appendix A, the Strategy is built around the practical outcomes that technology delivers for staff and communities across three core pillars.

4.3 Key Highlights of the Strategy

4.4 **Pillar 1:** Active Cyber Resilience focuses on protecting the critical services that residents rely on from digital threats and disruption. Building on the Councils' existing defences, this pillar prioritises strong, fast operational recovery so that essential community lifelines, such as Housing and Revenues & Benefits, can be restored quickly following any incident. By 2028, both Councils will have 24/7 smart network monitoring (Microsoft Sentinel) and advanced device protection (Microsoft Defender) active at £0k additional licence cost—rationalising security software into fewer systems by exiting separate Trend Micro and Mimecast contracts—alongside executive cyber governance under the Senior Information Risk Owner (SIRO), regular recovery and manual fallback drills tested with Business Continuity, and mandatory training for all staff and Members. By 2029, the Councils will be fully aligned with the Cyber Security and Resilience Bill and protected by locked, isolated data vaults as new Unitary Authorities go live.

4.5 **Pillar 2:** Data Intelligence & Ethical AI sets out how the Councils will transform corporate data into insight and deploy responsible, UK-hosted Artificial Intelligence (AI) to automate routine administration. Reflecting the Government's approach to public-sector AI, AI safety, and sovereign UK data centres set out in the Autumn Budget 2026, every tool will operate under strict UK Data Sovereignty and mandatory Human-in-the-Loop oversight, ensuring trained staff fact-check outputs and retain full accountability for any decision affecting a resident. By 2028, the Joint AI Governance Board and plain-English staff guidance under the Corporate AI Policy will be embedded, Microsoft 365 permissions and duplicate or outdated files (ROT data) will be tidied up, and supervised UK-hosted AI trials will support officers in Planning validation and Freedom of Information (FOI) requests. By 2029, historical records across departments will be cleansed so zero inaccurate or junk data is carried into future Unitary systems.

4.6 **Pillar 3:** Future-Ready Tech & Culture focuses on maintaining modern infrastructure, exploiting the full value of existing software before buying new systems, and empowering the workforce through targeted training and safe digital tools. Over the next 12 to 18 months, delivery under this pillar will be anchored by two shared flagship projects: replacing Corporate Telephony (Microsoft Teams and Mitel) to relieve pressure on the Customer Service Centre (CSC) and improve resident call handling, and replacing legacy Virtual Desktop Infrastructure (VDI) and "Zero-Client" desk terminals. By 2028, the service will also launch the SharePoint Corporate Intranet Hub, a two-year Microsoft 365 staff training programme, a Corporate Project Management Office (PMO), and an accurate central register of all Council

hardware and software (CMDB), before rationalising legacy software into fewer, more efficient systems by 2029.

4.7 To ensure the Strategy remains responsive during this period of structural change, the Joint ICT Committee will formally review the Strategy and its High-Level Action Plan. This rolling review mechanism ensures that both Councils can adjust priorities immediately upon a national announcement on LGR.

4.8 Consultation

4.9 The Strategy has been developed collaboratively across Stevenage Borough Council and East Herts District Council with input from senior leadership, service managers, Business Continuity, and the Business Change and Digital team. It is endorsed by the Portfolio Holder for Resources and Performance (Councillor Tom Plater) and the East Herts Executive Member (Councillor Joseph Dumont) and has been formally agreed by the Joint ICT Committee.

5 IMPLICATIONS

Financial Implications

5.1 There are no direct financial implications arising from the recommendations contained in this report. Core operational delivery of the Shared ICT Strategy 2027–2029 will be met within existing budgets, and any future projects requiring additional investment will be subject to individual Business Cases and the Council's standard financial approval processes.

Legal Implications

5.2 There are no direct legal or legislative implications arising from the recommendations contained in this report.

Local Government Reorganisation (LGR) Implications

5.3 Following the rapid review announced on 7 September 2026 and the ministerial update on 29 October 2026, the Government confirmed that the Local Government Reorganisation (LGR) process and criteria were sound, with shadow elections scheduled for 2028 and new Unitary Authorities set to go live in 2029, while Hertfordshire awaits a final decision before Christmas 2026 or early in the New Year. Built on the premise that LGR will proceed, the Strategy uses this window constructively to reduce technical debt, tidy corporate data, and design modular systems that can easily connect to partner networks or transition to a future Unitary Authority without service disruption—or, if LGR does not happen for an extended period, to go further with deeper system integration, rationalisation into fewer systems, and shared efficiencies. To ensure the Strategy remains responsive during this period of structural change, the Joint ICT Committee will formally review the Strategy and its High-Level Action Plan, ensuring that both Councils can adjust priorities immediately once the Government confirms its next steps on LGR. Risk Implications

5.4 There are no direct significant risks to the Council arising from the recommendations contained in this report

APPENDIX A:

ICT Strategy 2027–2029

Stevenage Borough Council & East Herts District Council

Secure Foundations, Intelligent Services, Empowered People



- **Table of Contents**

1. Table of Contents 5
2. Executive Summary: Building a Secure, Smart, and Agile ICT Service 6
4. Introduction: Our Shared Journey 9
5. Introducing the Three Pillars of the Strategy 10
6. Pillar 1: Active Cyber Resilience 12
7. Pillar 2: Data Intelligence & Ethical AI 16
8. Pillar 3: Future-Ready Tech & Culture 18
9. Resourcing the Vision 19
10. Appendix A: High-Level Action Plan (2027/ 2028) 21
11. Appendix B: Glossary of Strategic Terms 24

- **Executive Summary: Building a Secure, Smart, and Agile ICT Service**

The Councils' priority is delivering excellent, reliable services to the residents, staff, and officers of Stevenage Borough Council and East Herts District Council. As resident and staff expectations grow and the structure of local government changes, the technology the Councils use must evolve. This strategy ensures the shared ICT service continues to provide a responsive, agile service that supports Council staff and enables both Councils to adapt and grow.

Rather than focusing solely on software, this strategy is built on what technology delivers for Council staff and communities.

Our Vision for 2029

By the end of this strategy in 2029, the Councils will have built strong cyber security defences and fast recovery capabilities in the event of any disruption. The Councils will be working smartly to maximise the technology we have already invested in, particularly the Microsoft suite.

The Councils will have successfully adopted safe, ethical Artificial Intelligence (AI) tools to support Council staff. Most importantly, the Councils will be fully ready for the future, remaining agile to whatever happens next in technology or local government structures.

Keeping Resident Services Safe

Where the Councils Are Now: The Councils currently employ robust digital defences, including modern digital border controls (next-generation firewalls) and automated network monitoring, to safeguard resident data. The shared ICT service maintains secure, locked backups that cannot be altered or deleted (immutable backups) to protect against digital threats.

The Councils' Future Aspiration: The Councils will move beyond standard defence to achieve active cyber resilience, focusing on fast recovery from any disruption.

How the Councils Will Achieve This: The shared ICT service is deploying active network monitoring systems that act as smart alarms to stop suspicious activity immediately. This guarantees that critical community lifelines remain online and secure against evolving cybersecurity threats.

Working Smarter to Save Time

Where the Councils Are Now: The Councils have successfully migrated legacy systems to modern platforms and streamlined our online service forms.

The Councils' Future Aspiration: The Councils will unlock the full potential of existing tools, such as Microsoft 365 and Power BI, to help Council staff work smarter. The Councils will adopt responsible, UK-based AI tools to handle routine paperwork and automatically route standard service requests.

How the Councils Will Achieve This: The shared ICT service will run low-risk trials to prove the value of new digital tools before any wider release. The Corporate AI Policy governs oversight and sets safe boundaries to ensure Council staff use these

platforms securely and verify external data. This will allow staff to spend less time on manual administration and more time helping residents face-to-face.

Ready for the Future

Where the Councils Are Now: The Councils are preparing their digital estate for potential upcoming local government restructuring. Following the rapid review announced on 7 September 2026 and the ministerial update on 29 October 2026, the Government confirmed that the Local Government Reorganisation (LGR) process and criteria were sound, with shadow elections scheduled for 2028 and new Unitary Authorities set to go live in 2029. With the previous July decision withdrawn, Hertfordshire awaits a final decision before Christmas 2026 or early in the New Year following further testing of existing proposals. Both Councils are collaborating closely with Hertfordshire partner Councils to align technology standards.

The Councils' Future Aspiration: This strategy is built on the premise that LGR will proceed. While the final outcome or timing of LGR for Hertfordshire is still in the waiting stage, this window gives the Councils the potential time and capacity to design flexible systems that can adapt to whatever future structure is decided on. However, if LGR does not happen for an extended period, the Councils will use this foundation to go further with deeper system integration, rationalisation into fewer systems, and shared efficiencies.

How the Councils Will Achieve This: The shared ICT service will use this extra capacity to audit technical debt and build flexible, modular foundations where appropriate, ensuring no drop in service quality during any future transition. The Councils will prepare the groundwork while recognising that the final structure of services will ultimately be led by the future Unitary Authorities if the merger goes ahead.

The Challenge: A Period of Historic Transformation

Local government is balancing rapid technological advances, rising expectations from residents, and upcoming structural reforms. The Councils are managing these significant changes while carefully controlling budgets.

The Rise of Smart Technology: Everyday technology is advancing quickly, and residents rightly expect services to be faster and available around the clock. The Councils are maximising core platforms we already own, such as Microsoft 365 and corporate reporting tools like Power BI. The Councils will empower Council staff with the right tools and training so they can confidently use technology to deliver better support to our community.

Navigating Local Government Reorganisation (LGR): Local government in England is exploring a transition into single unitary organisations. The Councils will collaborate closely across Hertfordshire Councils to ensure systems connect smoothly and legacy data remains safe. Council business will continue without interruption, whether running on existing platforms or transitioning to new unitary systems.

The Solution: Three Pillars for Success

To meet these challenges, the Council's technology strategy is built around three core pillars.

Pillar 1: Active Cyber Resilience

Where the Councils Are Now: The Councils currently protect resident data using standard perimeter defences to block digital threats.

The Councils' Future Aspiration: The Councils are advancing beyond standard protection to build strong and fast recovery capabilities. If a digital attack happens, we guarantee that critical lifelines—such as Housing and Revenues & Benefits—can be brought back online for communities as fast as possible.

Pillar 2: Data Intelligence & Ethical Smart Tools

Where the Councils Are Now: The Corporate AI Policy will ensure any new technology is governed with the same care and rigour as our human workforce.

The Councils' Future Aspiration: The Councils are actively exploring and piloting secure, UK-based automated tools to lift the burden of repetitive administrative tasks from Council staff. We ensure every digital decision remains safe, ethical, and focused on the resident.

Practical Case Study: For example, the shared ICT service is actively exploring safe Artificial Intelligence (AI) solutions to assist with processing Freedom of Information (FOI) requests. This tool would quickly scan historical records and summarise relevant data, saving officers hours of manual searching.

Pillar 3: Future-Ready Tech & Culture

Where the Councils Are Now: The Councils provide staff with foundational training to confidently embrace new ways of working.

The Councils' Future Aspiration: The shared ICT service is designing flexible technology that can easily adapt and merge with other Councils' systems. This ensures the new unitaries in Hertfordshire can provide digital services from day one without any drop in quality.

Practical Example: The Councils are building modular, independent systems using platforms like GovService. By keeping these digital forms separate from older, tangled databases, they can be easily picked up and moved to any new Unitary Authority without breaking or causing service downtime.

- **Introduction: Our Shared Journey**

Since the ICT Partnership was formed in 2013, Stevenage Borough Council and East Herts District Council have worked together to provide shared technology support. The digital world moves fast, and the shared ICT service is shifting from a traditional IT support desk into a responsive service that actively improves Council delivery.

Strategic Alignment: The Foundation of Digital Transformation

This strategy serves as the technical bedrock for the **Stevenage Borough Council Digital Strategy 2025–2028**. While the Digital Strategy defines what interactions residents experience—such as online forms, AI chatbots, and automated telephony—this ICT Strategy defines how they are delivered safely.

It provides the reliable data protection and secure platforms needed to turn digital ambitions into everyday reality. We act as a strategic partner for the internal Business Change and Digital Teams to deliver accessible services across both Councils.

How this aligns key topics between both strategies:

- Shared Platform Development: We support the GovService digital platform, Microsoft 365 integration, and secure cloud hosting for core systems like Housing (NEC) and Revenues & Benefits.

- Artificial Intelligence & Governance: We connect our Cyber Security controls directly to the Digital Strategy's AI goals under a joint Corporate AI Policy.

- Joined-Up Delivery: We align our technical delivery with the Business Change and Digital Board, ensuring system integration and security rules operate smoothly.

A Period of Historic Change

Where the Councils Are Now: Both Councils are navigating rapid technology changes while preparing for the potential transition of Stevenage Borough Council and East Herts District Council into new unitary bodies, subject to the rapid review and revised timeline for LGR. The Councils' immediate priority is ensuring day-one operations remain safe, legal, and operational without destabilising shared services.

The Councils’ Future Aspiration: Built on the premise that LGR will proceed, the Councils will use the potential time available before restructuring ahead of 2028 shadow elections and 2029 Unitary go-live to build upon current systems and thoughtfully design future connections between Councils, while recognising that the final structure of the service will ultimately be led by the future Unitary Authorities. If LGR does not happen for an extended period, the Councils will go further in rationalising and integrating systems across the shared service to drive deeper efficiencies.

To manage this complex transition seamlessly, our Councils' priorities are:

- **Connecting Council Systems:** Bringing together different networks so staff can collaborate securely from anywhere.
- **Creating a Single Version of the Truth:** Reviewing duplicate systems to ensure Council data is accurate, easy to find, and saves the Council money.
- **Moving Data Safely:** Ensuring that when we transfer resident records or archive legacy databases, they are handled with the highest level of security.
- **Unifying Defences:** Creating shared Cyber Security rules across **Hertfordshire** authorities to protect merged organisations from digital threats.
- **Keeping Services Running:** Ensuring staff and residents experience zero disruption to critical systems.
- **Supporting Our People:** Helping staff confidently adapt to new, digital-first ways of working.

Building on Solid Foundations

Where the Councils Are Now: To fix historic underinvestment, both Councils have invested £630,000 per annum since 2023/24 to address obsolete systems. This has enabled the shared ICT service to fully replace outdated networks and to build a secure digital environment.

Key achievements include:

- **Infrastructure Modernisation:** The shared ICT service successfully migrated to Windows 11, ensuring both Councils are operating on the most recent and modern infrastructure.
- **Resilience Upgrades:** The shared ICT service implemented high-speed data storage arrays and next-generation firewalls. This means Council systems run faster, Council data is secure, and residents experience zero downtime during essential Council maintenance.
- **Workforce Enablement:** The shared ICT service rolled out Microsoft 365 to all staff so colleagues can access systems remotely, collaborate easily, and share data securely. However, we recognise that installing the software is just the start of our journey to working smarter, and further work in rolling out our Microsoft 365 architecture and staff training is required.

The Councils' Future Aspiration: Using advanced software and automation requires a reliable foundation. The Councils will ensure Council systems remain reliable and available, apply regular security patches, and get more value from tools like Microsoft 365 and NEC Housing, where interfaces have recently been tested and integrated. With these foundations in place, the shared ICT service is shifting its focus from basic IT fixes toward actively improving the digital services we deliver to communities every day.

- **Introducing the Three Pillars of the Strategy**

The following pages define the three core pillars that will guide the ICT work programme between 2027 and 2029.

- **Active Cyber Resilience:** Protecting the services residents rely on from digital threats and disruption.
- **Data Intelligence & Ethical AI:** Transforming data into insight and deploying responsible, UK-hosted AI tools to automate routine tasks. The Councils will achieve this by running safe, low-risk trials of digital assistants to help staff process heavy paperwork, such as Freedom of Information (FOI) requests.
- **Future-Ready Tech & Culture:** Building a flexible technology estate and a culture of continuous learning ready for the next decade. By flexible, this means building modular systems that act like independent building blocks. These systems can easily plug into partner networks or cleanly detach if Council boundaries change, ensuring our technology adapts without breaking.

- **Pillar 1: Active Cyber Resilience**

Active Cyber Resilience: Protecting the services our residents rely on from digital threats and disruption

Goal: Protecting the services residents rely on from digital threats and disruption.

In an increasingly digital world, online threats are a matter of "when," not "if". Hostile actors increasingly deploy sophisticated cyber operations to disrupt critical public infrastructure. In the past twelve months, both Councils have experienced five state-sponsored cyber-attacks.

Despite this substantial escalation, the Councils' existing security measures successfully prevented 480,000 malicious attempts in a single quarter. Building directly on these strong current defences, our strategy will now focus on rapid recovery. The Councils will ensure we can withstand attacks, keep resident data safe, and restore critical services at speed.

The Council's Eight Biggest Cyber Threats: Rather than focusing purely on the technical mechanisms, the Council views these eight primary threats through the lens of how they impact our ability to serve the community:

- **System Overloads (Denial-of-Service):** Attacks that intentionally flood the network with fake traffic to crash Council systems, making it impossible for residents to access online Council services. The Councils' Solution: The shared ICT service uses smart traffic filters that act like border guards, instantly spotting and blocking fake traffic before it can crash the Council's sites.
- **Third-Party Vulnerabilities (Supply Chain Attacks):** Hackers are attempting to bypass our security by breaking into the external suppliers, vendors, and partners connected to the network. The Councils' Solution: The shared ICT service will conduct strict security checks on all suppliers and limit their access to only what is necessary for their jobs.
- **New and Evolving Threats:** The constant, rapid development of new cyber-attack methods requires the security teams to remain highly adaptable and vigilant. The Councils' Solution: The shared ICT service will use automated alarm systems that monitor the network 24/7 to detect unusual activity instantly and alert partner Councils.
- **Software Weak Spots (Unpatched Vulnerabilities):** Outdated software acts like an unlocked door, giving attackers an easy route into the network if security updates are not applied immediately. The Councils' Solution: The shared ICT service will automatically push out regular security updates across all staff computers and systems to lock those doors immediately.
- **Digital Blackmail (Ransomware):** Malicious software that locks the Council's systems and demands payment to restore access, severely disrupting critical

daily work such as housing support or benefits processing. The Councils' Solution: The shared ICT service will maintain immutable, offline backups of Council data in secure digital vaults, allowing us to restore Council systems quickly without ever paying a ransom.

- **Tricking Council Staff (Phishing):** Highly deceptive emails or messages designed to manipulate Council employees into inadvertently handing over passwords or secure access. The Councils' Solution: The shared ICT service will run regular cybersecurity training and practice drills for all staff and Members, so everyone knows how to spot and report suspicious emails.
- **Resident Data Theft (Data Breaches):** The theft or accidental exposure of sensitive personal information can cause severe financial and emotional harm to the community we serve. The Councils' Solution: The shared ICT service will scramble (encrypt) all private data so that even if someone intercepted it, it would be completely unreadable to them.
- **Internal Risks (Insider Threats):** Accidental errors or unauthorised actions by staff, which we actively prevent through careful system monitoring, strict access controls, and training. The Councils' Solution: The shared ICT service will grant staff access only to the specific files they need for their role and continuously monitor system usage to catch mistakes early.

To achieve the Active Cyber Resilience goal of protecting essential resident services from digital threats and disruptions, the Councils will:

Local Government Reorganisation (LGR): A Unified Hertfordshire Baseline

As the Councils prepare for possible local government restructuring, we must align our cyber defences with all other Councils in Hertfordshire. Cyber threats do not respect regional borders; a weakness in one Council can threaten the wider county network.

The Councils will establish a shared security baseline with our neighbouring Councils. This guarantees that all residents receive the same high standard of protection against cyber-attacks, regardless of their local authority. To achieve this unified baseline, the Councils will meet an agreed cyber standard, standardise our policies, and build a rapid-alert network to share live threat data across Hertfordshire, fully aligning with the upcoming Cyber Security and Resilience Bill (2025).

Enhanced Cyber Defences

The Councils currently rely on standard perimeter protection to block external threats. To advance these defences, the shared ICT service will be installing advanced security technologies that act as smart burglar alarms and digital security cameras for the network.

Instead of passive firewalls, these modern defences actively monitor traffic to instantly detect and block suspicious activity before it reaches resident data. The Councils will also deploy automated tools to analyse security alerts across our entire network in real-time, allowing us to spot new attack methods instantly.

Furthermore, the Councils will create secure, isolated vaults within Council systems. This ensures that if one area is compromised, the breach cannot spread to critical services.

Incident Response Simulations and Recovery Testing

Defence alone is not enough; true resilience requires the Councils to recover from major disruptions with confidence. Working closely with Business Continuity teams, the Councils will establish a regular schedule of Incident Response Simulations and disaster recovery drills involving technical teams, leadership, and frontline service managers.

These drills test our ability to restore essential services, like Housing and Revenues and Benefits, within agreed timeframes. Working with Business Continuity, the Councils will support service teams to rehearse manual fallback procedures—such as Revenues and Benefits practising how to process an emergency resident payment using temporary pen-and-paper procedures during a simulated computer outage.

Cybersecurity Awareness & Culture:

Safeguarding the organisation requires a human firewall where every staff member is empowered to recognise and respond to threats. The Councils currently provide basic cybersecurity training, but the Councils will expand this into a mandatory training programme covering the latest best practices and secure remote working habits.

Staff will participate in safe, simulated phishing exercises. To ensure this is a valuable learning experience, the Councils will provide immediate, constructive feedback rather than just testing our teams.

The Councils will foster a supportive environment where staff are encouraged to report incidents and near-misses without fear of blame. This approach turns every employee into an active, informed line of defence.

Incident Response Protocols:

The shared ICT service will maintain clear, step-by-step incident response plans alongside Business Continuity, so every staff member knows their exact role if an attack happens. This structured approach ensures swift, coordinated action to contain threats, minimise service disruption, and meet national regulatory standards.

What Success Looks Like by 2028 and 2029

By 2028, both Councils will have 24/7 smart network monitoring (Microsoft Sentinel) and advanced device protection (Microsoft Defender) active at £0k additional licence cost—rationalising security software into fewer systems by exiting separate Trend Micro and Mimecast contracts—alongside regular recovery drills tested with Business Continuity. By 2029, the Councils will *be fully aligned with the Cyber Security and Resilience Bill and protected by* locked, isolated data vaults, ensuring community lifelines remain protected and resilient as new Unitary Authorities go live.

- **Pillar 2: Data Intelligence & Ethical AI**



Goal: Transforming data into insight and deploying responsible, UK-hosted AI to automate the routine.

Data is the foundation of everything we do, and AI offers significant potential to streamline tasks and support Council staff.

Where the Councils Are Now: Both Councils currently still rely on some manual processing for routine administrative tasks. Recognising the acceleration of AI capabilities and that Council staff may look for AI solutions, our joint Corporate AI Policy will set safe boundaries for any modern technology. The Councils' Future Aspiration: The Councils will not try to be at the forefront of AI development. Instead, the Councils will learn from other organisations and test proven solutions in low-risk environments to assess their accuracy before any wider deployment.

Ethical AI and UK-Hosted Cloud Systems

Where the Councils Are Now: The Councils currently apply the highest standards of accountability to our human staff and securely manage existing data.

The Councils' Future Aspiration: As the Councils look to move systems into the cloud, they will not use a one-size-fits-all approach. The Councils will only migrate systems when there is a clear business case proving it is the most secure, reliable, and cost-effective option for that specific service.

Crucially, whether the Councils are deploying new AI tools or moving existing databases to the cloud, everything must be hosted entirely within the United Kingdom. This strict requirement directly reflects the Government's new approach to public-sector AI, AI safety, and sovereign UK data centres set out in the Autumn Budget 2026, ensuring that all resident data remains securely within national borders and is fully protected by UK privacy laws.

Practical Examples of Automation

To provide concrete examples of how this technology will be used, the Councils are focusing on lifting the burden of repetitive administrative tasks from support departments.

Practical Example: Routine planning applications could be processed using a smart digital assistant. This tool would verify that standard forms are attached and automatically log the details into our planning system, freeing support officers from manual data entry so they can spend more time helping residents navigate complex queries.

Human-in-the-Loop Governance

Where the Councils Are Now: The Corporate AI Policy will establish clear ethical standards for every tool the Councils deploy.

The Councils' Future Aspiration: The Councils' approach is to enhance human oversight, not replace it, by keeping a 'Human-in-the-Loop'. While digital systems will process data and propose actions, any decision affecting a resident's access to services, financial situation, or wellbeing will always remain under the direct supervision of trained staff.

Unlike traditional software—which is tested thoroughly before launch so that it produces the exact same output every time—AI tools can generate different outputs and may occasionally be inaccurate. Because of this, the Corporate AI Policy makes fact-checking mandatory, and a human will review required actions where necessary to ensure trust, legal compliance, and clear accountability.

Governance of the Digital Workforce (IT as Digital HR)

Where the Councils Are Now: The shared ICT service currently manages standard software procurement and licensing.

The Councils' Future Aspiration: The shared ICT service will explore Smart Digital Assistants, such as Microsoft Copilot, to act as extra hands for our officers. As we integrate these tools, the ICT department will act as Digital HR, managing the entire lifespan of the digital workforce to guarantee they align with our values.

The main components of this digital governance are:

- **Procurement (Recruitment):** Every new AI tool follows a strict recruitment process, just like hiring new staff. This includes rigorous checks to ensure the tool makes fair, unbiased decisions using secure, enterprise-grade systems.
- **Monitoring (Performance Management):** The shared ICT service will track their accuracy and fairness in real-world scenarios. Automated alerts will flag any unexpected behaviour, and staff will have clear ways to provide feedback on system performance.
- **Decommissioning (Offboarding):** When a digital tool fails to meet our high standards, the Councils will securely remove the system, instantly revoke all network access, and ensure all associated data is safely deleted.

Preparing for Local Government Reorganisation (LGR)

Where the Councils Are Now: Both Councils hold vast amounts of historical data across disparate Council departments.

The Councils' Future Aspiration: To support any potential upcoming merger of local Councils, the Councils will establish clear stewardship roles to thoroughly cleanse existing data. By standardising how we store information now, we prevent the transfer of inaccurate or junk data. This guarantees that from day one, Council staff can instantly find the reliable information they need to make good decisions for residents.

What Success Looks Like by 2028 and 2029

By 2028, the Joint AI Governance Board and plain-English staff guidance will be embedded, Microsoft 365 file permissions and duplicate, outdated, or unnecessary files will be tidied up with sufficient guardrails, and supervised UK-hosted AI trials will be delivering administrative efficiencies in Planning validation and Freedom of Information (FOI) requests. By 2029, the Councils will have cleansed historical records across departments and established trusted Human-in-the-Loop automation, saving officer hours on routine data entry and ensuring zero inaccurate or junk data is carried into future Unitary systems.

- **Pillar 3: Future-Ready Tech & Culture**



Goal: Building a flexible technology estate and a culture of continuous learning ready for the next decade.

To meet the evolving needs of residents, both Councils must remain agile. The Councils' technology approach focuses on maintaining modern infrastructure, exploiting the tools we already own, and supporting our people.

Operating on Modern Infrastructure and Maximising Functionality

Now that our ICT service is fully staffed and both Councils have invested in core systems, our aim is to ensure that the core software is kept up to date with the latest supported versions. This approach reduces security risks and prevents a new build-up of outdated technical debt.

Before buying any new software, the Councils' default approach is to look at what we already have and **exploit the full value** of the digital tools we already pay for. The shared ICT service will unlock unused features within our current platforms through routine licence reviews, shared software discovery sessions, and cross-departmental best practice forums to improve data sharing and save taxpayer money.

Empowering Staff to Build Safe Digital Tools

Platforms like GovService and low-code tools in Microsoft 365 (such as Power Apps and Power Automate) allow trained staff with little to no coding experience to build simple digital forms and automated workflows.

Working across the Business Change and Digital Team and the ICT department, the Councils will support service areas to design solutions that work for their teams. To keep Council systems secure, ICT will put sufficient guardrails and safe, approved environments in place, so new workflows meet our security standards and avoid creating an unmanageable tangle of unsupported apps.

Cost-Effective, UK-Based Hosting and Restructuring

When deciding where the Councils' systems and data will live, we focus purely on the business case to find the most secure, reliable, and cost-effective home for that specific service. Regardless of the technical setup we choose, all our solutions will be hosted entirely within the UK. This ensures residents' sensitive data is strictly protected by UK privacy laws (GDPR) and remains under the highest standards of legal governance.

Workforce Empowerment & Continuous Learning

The Councils' success depends entirely on our people, and we want our employees to be empowered, proactive participants who drive our transformation. The Councils will give the workforce the time, resources, and training they need to adapt to changing demands. This includes tailored workshops, online learning platforms, and mentoring schemes designed to enhance digital literacy and build confidence.

To support this, the Councils will invest in dedicated IT trainers who can create bespoke training packages for Council staff. For example, our aim is that a service officer will learn to fully utilise Microsoft 365 tools and write safe AI prompts in compliance with the Corporate AI Policy. By using these new skills to quickly summarise lengthy documents, they safely eliminate hours of administration, allowing them to spend more time directly helping residents.

What Success Looks Like by 2028 and 2029

By 2028, the shared ICT service will work with the Councils to upgrade to the latest versions of systems, alongside delivering better online services and a modernised Microsoft Teams and Mitel phone system for residents, replacing ageing "Zero-Client" desk terminals, and launching the SharePoint Intranet Hub, two-year staff training programme, Corporate PMO, and an accurate central register of all Council hardware and software. By 2029, the Councils will have rationalised legacy software into fewer, more efficient systems and empowered a digitally confident workforce ready for Unitary transition without service disruption.

- **Resourcing the Vision**

Clarifying Investment vs. Operational Delivery To ensure financial prudence and transparency, this strategy clearly distinguishes between daily operations covered by the Councils' existing shared IT budget and new projects requiring strategic investment.

- **Core Deliverables (Within Existing Resources):** Doing the basics well, including keeping systems online, applying security patches, getting the most out of existing tools (like Microsoft 365 and NEC Housing), and providing standard cybersecurity training, will all be delivered within the existing base budget.
- **Strategic Enhancements (Investment Required):** Transformational projects—such as procuring targeted AI licenses (like Microsoft Copilot) for staff under AI Policy governance oversight or undertaking major system redesigns—will be subject to individual Business Cases. These initiatives must

demonstrate a clear Return on Investment (ROI), a statutory necessity, or essential readiness for Local Government Reorganisation (LGR) before funding is released.

- **Social Value in Procurement:** All strategic investments will be evaluated not only on their financial ROI but on Social Value. This ensures that the Councils' technology supply chain actively supports local economic growth and provides tangible community benefits.

Alignment with Corporate Priorities

This strategy is not a standalone IT document; it is the technical enabler for the high-level corporate ambitions of both Councils.

Stevenage Borough Council: "Making Stevenage Even Better"

- **Transforming Our Town:** The Council's commitment to Future-Ready Tech (Pillar 3) ensures that the Council's digital infrastructure is scalable and robust enough to support the town's major regeneration programmes and the £1bn investment agenda.
- **Thriving Neighbourhoods:** By delivering Active Cyber Resilience (Pillar 1), we protect the critical services and sensitive data that residents rely on, ensuring community trust and safety are maintained.
- **Technology & Innovation (Cross-Cutting Theme):** As highlighted in the Corporate Plan, technology is a cross-cutting theme. This strategy delivers the "Ethical & UK-Hosted AI" and "Asset Optimisation" required to drive efficiency across all services.

East Herts District Council: "L.E.A. F" Priorities

- **L – Listening, Open and Transparent:** The Data Intelligence pillar (Pillar 2) provides the accurate evidence base required to improve consultation and ensure decision-making is open and transparent.
- **E – Environmentally Focused:** By prioritising Asset Optimisation and extending hardware lifecycles (Pillar 3), we directly support the Council's aim to reduce carbon emissions and operate sustainably.
- **A – Acting with the Community:** Our focus on Social Value in Procurement ensures that our technology spend supports the local voluntary sector and businesses, helping to create thriving high streets and communities.
- **F – Fair and Inclusive:** Through Workforce Empowerment and accessible systems (Pillar 3), we support the delivery of fair services. A secure, resilient IT estate allows the Council to support vulnerable residents effectively, from homelessness services to Council Tax Support.

- **Appendix A: High-Level Action Plan (2027/ 2028)**

This Action Plan translates the ICT Strategy into a clear, phased delivery programme across Stevenage Borough Council and East Herts District Council. It breaks down our strategy into manageable phases across our three core pillars over the next three years.

To ensure the strategy remains responsive during a period of structural change, the Joint Information and Communications Technology (ICT) Committee will move to twice-yearly meetings and formally review this work plan every six months. This rolling six-month review cycle guarantees that if a national announcement is made on Local Government Reorganisation (LGR), both Councils can adjust priorities immediately without stalling delivery.

Across the next 12 to 18 months, our portfolio is anchored by two shared strategic projects that will transform daily operations for staff and residents across both authorities:

1. **Replacing Corporate Telephony**: Delivering a modern Unified Communications (Microsoft Teams and Mitel) telephony platform to relieve pressure on frontline call handlers and transform the resident contact experience.
2. **Replacing the Virtual Desktop Infrastructure (VDI) and "Zero-Client" Terminals:** Retiring ageing desktop terminals ("Zero boxes") and old central virtual desktop servers (Virtual Desktop Infrastructure / VDI), moving staff onto reliable modern laptops and equipping field officers with mobile tablets suited to their roles.

2. Core Annual Activities (Completed Every Single Year)

Alongside phased project milestones, the shared service will complete five foundational operational activities every year to keep Council staff, systems, and democratic processes ready:

- **Continue Mandatory Cybersecurity Training**: Deliver annual cybersecurity and secure remote-working training for all Council employees, reinforced by targeted training for high-risk teams.
- **Run Simulated Phishing Exercises**: Send regular, safe test phishing emails to **staff and Members** to build scam awareness, providing immediate, constructive learning feedback rather than blame.
- **Conduct Incident Response and Disaster Recovery (DR) Simulations**: Run multi-service scenario exercises where technical teams and leadership practice restoring critical lifelines—such as Housing and Revenues and Benefits—within pre-agreed Recovery Time Objectives (RTOs).
- **Work with Business Continuity on Manual Fallback Operations:** Working with Business Continuity teams, support frontline departments to rehearse temporary pen-and-paper procedures so essential support for vulnerable residents continues during any extended digital outage.

- **Deliver Democratic and Elections Technology Support**: Provide dedicated network resilience, equipment readiness, and out-of-hours technical support for all by-elections and all-out local elections across both Councils.

Active Cyber Resilience: Protecting the services our residents rely on from digital threats and disruption

Year 1 (2027/28): Foundation, Active Monitoring and Cyber Assessment Framework (CAF) Phase 1

- **Mobilise Executive Cyber and Risk Boards:** Launch the ICT Risk Board and the Joint Stevenage and East Herts Security Board under the oversight of Councils' board-level executive responsible for data security (Senior Information Risk Owner / SIRO), aligning security policies across Hertfordshire.
- **Exploit Existing Microsoft Security Licences (Saving on Duplicate Software):** Switch on the automated security alarm system (Microsoft Sentinel) and advanced computer protection (Microsoft Defender) already included in the Councils' Microsoft contract at £0k additional licence cost. This allows us to exit our separate antivirus contract (Trend Micro) and retire our separate third-party email filtering tool (Mimecast) by consolidating email protection into Microsoft 365 Defender.
- **Deploy Active Network Defences (Cyber Assessment Framework Phase 1):** Set up a central security monitoring dashboard that watches for suspicious activity (Service Integration and Management / SIAM Event Monitoring), divide the central data centre network into separate locked zones so a breach cannot spread (Datacentre Network Segmentation), and enforce automated device protection rules to block suspicious traffic in real time.
- **Upgrade Ageing Back-Office Servers:** Begin the multi-year migration off ageing Windows Server 2019 systems alongside cross-departmental Disaster Recovery (DR) scenario testing.
- **Complete Cyber Assessment Framework (CAF) Phase 2 and National Cyber Security Centre (NCSC) Readiness:** Tighten controls over who can access data in Microsoft 365, carry out security checks on external software suppliers (supply chain risk assessments), audit digital border rules (firewalls), and document two-step login verification rules (Multi-Factor Authentication / MFA conditional access).

Data Intelligence & Ethical AI: Transforming data into insight and deploying responsible, UK-hosted AI to automate the routine

Strategic Goal: Transforming data into insight and deploying responsible, United Kingdom (UK)-hosted Artificial Intelligence (AI) to automate routine administration.

Year 1 (2027/28): Data Guardrails, Warehouse Foundation and Staff Guidance

- **Create AI Policy Guidance and Establish the Joint Governance Board:** Publish clear, plain-English staff guidance on the Corporate AI Policy, and establish a joint AI Governance Board across Stevenage Borough Council and East Herts District Council.
- **Put in Sufficient Guardrails for Microsoft 365 Architecture and Permissions:** Finalise the Microsoft 365 security design, apply automatic security tags to confidential documents (Data Protection Sensitivity Labels), catalogue archived records, and run a shared file tidy-up pilot to remove duplicate, outdated, or unnecessary files (Redundant, Obsolete, or Trivial / ROT data) so clear access rules are enforced before scaling new tools.
- **Trial Low-Risk Line-of-Business Automation:** Run supervised trials of UK-hosted AI tools to assist officers with checking routine Planning Applications and scanning documents for Freedom of Information (FOI) requests.



Future-Ready Tech & Culture: Building a flexible technology estate and a culture of continuous learning ready for the next decade

This work plan outlines how the Councils will build a flexible technology estate and a culture of continuous learning. It prioritises optimising our current assets and using **LGR** delay to professionally design future systems.

Year 1: Audit, Governance & Foundation

- **Shared Strategic Project – Replace Corporate Telephony:** Procure and roll out a unified phone and contact centre platform (Microsoft Teams and Mitel) to relieve pressure on the Customer Service Centre (CSC) and improve resident call handling.
- **Shared Strategic Project –** Replace Virtual Desktops (VDI) and Zero-Client Hardware: Approve and deliver the business cases to replace legacy central desktop servers (Virtual Desktop Infrastructure / VDI) and retire end-of-life desk terminals (Zero-Clients), moving staff onto modern laptops and tablets.
- **Launch the "Microsoft 365 Exploitation" and Staff Training Programme:** Recognising that further work is needed to roll out Microsoft 365 fully, deliver a new staff intranet website (SharePoint Corporate Intranet Hub), complete phased departmental Microsoft 365 rollouts, and run a two-year staff training programme to get the most out of the Councils' existing tools.
- **Strengthen Project Tracking and Staff Digital Skills:** Establish a consistent way of tracking and reporting on technology projects (Corporate Project

Management Office / PMO), bring in dedicated IT Trainers, and complete the Corporate Digital Skills Survey so training matches staff needs.

- **Mature Our IT Service Management (ITSM) and Configuration Management Database (CMDB):** Building on the single IT helpdesk portal, the shared ICT service will standardise how we manage and track IT support, system changes, and service requests (Information Technology Service Management / ITSM) and build an accurate central register of all Council hardware, software, and system connections (Configuration Management Database / CMDB).

- **Appendix B: Glossary of Strategic Terms**
  To assist in reviewing this strategy, the following technical terms and concepts are defined in plain English below:

  - **SIRO (Senior Information Risk Owner):** A mandatory board-level role within a Local Authority. The **SIRO** is the Executive Director responsible for managing information risk and ensuring the Councils' data assets are protected.
  - **Virtual Desktop Infrastructure (VDI):** A technology that hosts a user's Windows screen, files, and apps on a central server rather than on a physical laptop. The Councils are replacing our legacy VDI setup and desk terminals with modern, encrypted laptops and tablets.
  - **Staff-Led Digital Tools (Low-Code / No-Code):** A visual approach to building digital forms and workflows. This allows trained staff with little to no coding experience to create workflows using safe, approved drag-and-drop tools like **GovService** and **Microsoft Power Platform**.
  - **Artificial Intelligence (AI):** Computer systems that process data to help with tasks that normally require human effort, such as summarising documents, spotting trends, or routing routine forms.
  - **Ethical AI & Human-in-the-Loop:** AI systems deployed with fairness, transparency, and clear human oversight. Because AI outputs can vary—unlike traditional software that is tested to give the exact same result every time—a human officer reviews required actions **where necessary** so decisions remain accurate, safe, and accountable.
  - **Immutable Backups:** A secure type of data backup that cannot be altered, encrypted, or deleted for a set period, even by a system administrator. This is the Councils' critical defence for restoring systems after a ransomware attack.
  - **Council Merger / Local Government Reorganisation (LGR):** The potential process of transitioning from a two-tier Council system into a single-tier **Unitary Authority**. For the ICT service, this requires preparing flexible systems, clean data, and aligned security standards.

- **Recovery Timeframes (Recovery Time Objective / RTO):** The target maximum time within which a service must be restored after a cyber incident or outage. This strategy focuses on achieving strong and fast recovery for critical services like **Housing** and **Revenues and Benefits**.
- **Technical Debt (Legacy Debt):** The extra cost and risk caused by keeping outdated software or ageing hardware running instead of modernising it. Clearing this debt—such as replacing old telephony or legacy servers—is essential to keep services reliable.
- **API (Application Programming Interface):** A secure connector that allows different software programs to talk to each other automatically—such as connecting **NEC Housing** and **Finance** databases—without staff re-typing information.
- **UK Data Sovereignty:** The rule that all Council and resident data is hosted strictly within the **United Kingdom,** so it is governed by UK laws and fully protected under **UK GDPR**.
- **Smart Digital Assistants (Large Language Models / LLMs):** AI tools (such as **Microsoft Copilot**) trained to summarise documents, draft text, and help with routine admin while remaining under clear human oversight.